Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2015 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2015

Integrating Social and Economic Models of Responding to Privacy Messages in Mobile Computing: A Research Agenda

Dennis Galletta
University of Pittsburgh

David Eargle
University of Pittsburgh

Shadi Janansefat
University of Pittsburgh

Dimitar Kunev
University of Pittsburgh

Shivendu Pratap Singh
University of Pittsburgh

Integrating Social and Economic Models of Responding to Privacy Messages in Mobile Computing: A Research Agenda

Dennis Galletta
University of Pittsburgh, Pittsburgh, Pennsylvania, USA {galletta@katz.pitt.edu}

David Eargle
University of Pittsburgh, Pittsburgh, Pennsylvania, USA {dave@daveeargle.com}

Shadi Janansefat
University of Pittsburgh, Pittsburgh, Pennsylvania, USA {shj35@pitt.edu}

Dimitar Kunev
University of Pittsburgh, Pittsburgh, Pennsylvania, USA {dgk12@pitt.edu}

Shivendu Pratap Singh
University of Pittsburgh, Pittsburgh, Pennsylvania, USA {shs161@pitt.edu}

ABSTRACT

Mobile computing has provided technology to an unprecedented user base and has created a market for applications that is expected to reach $77 billion by 2017, involving over 268 billion downloads. Nearly every download involves privacy messages that request permissions to access information such as contact, calendar, and location information. Recent cases have revealed that users are often surprised when they discover the permissions they have granted, which implies that not everyone reads them carefully. In this paper we propose a research agenda focusing on the decisions that users make about those permissions requests. Several theories provide promising antecedents to explain acceptance of privacy permissions. Nine propositions are presented, with three from each research bases from social, economic, and cognitive perspectives. The research agenda thus is a combination hybrid social/economic/cognitive approach. The agenda complements extant research that has focused on privacy calculus theory.

Keywords: privacy, app permission requests, mobile computing, social influence theory, prospect theory, compliance-gaining strategies

INTRODUCTION

The proliferation of mobile computing is undeniable. The total size of the mobile app market is predicted to reach $77 billion by 2017 (Clifford, 2014), up from $26 billion in 2013 and $18 billion in 2012. In 2012, 11% of the revenues came from in-app purchases. That share is expected to reach 17% in 2013 and 48% by 2018 (Gartner 2013). In 2014, the two dominant markets, Apple's App Store and Google's Play Store, had more than 1.2 million apps each and second tier markets like Amazon's and Microsoft's each had roughly 300,000 apps (Bell 2015; Statista 2015). Furthermore, Gartner (2013) predicts that number of downloads in 2017 would nearly double the 2014 number, reaching 268.7 billion. A recent Nielsen report (2014) also pointed to increasing usage of mobile apps, both in terms of number of apps and time spent on them. Vendors, developers, and users alike find apps to be of great interest, attracting both time and money in large quantities.

There are many benefits and services provided by apps. However, apps are not without significant costs, even though 90% of all downloads are free (Gartner 2013). One of the most significant potential costs of using an app is that of permissions to access private data either stored on, or accessible to, the device. While these requests enable users to benefit from using the mobile app, they also open the door to security and privacy concerns. Privacy issues related to mobile apps are gaining prominence among researchers, practitioners and users as an important factor accompanying their adoption and continued use of the apps (Smith et al. 2011; Sutanto et al. 2013). In a study that measures the risks posed by mobile apps, the result of analyzing permissions requested by 528,433 apps on Google Play indicates that 46% of the apps collect between 1 and 20 sensitive permissions.

Practitioners have observed that the most common reason for apps to request (additional) permissions does not enable new or core functionality. Rather, it is to collect user and device

data that is later monetized through third parties (Greenberg 2014). A well-publicized case that illustrates some the potential issues is that of The Federal Trade Commission (FTC) v. Golden-shores Technologies, LLC and Erik M. Geidl (The Federal Trade Commission 2014). In this case, one of the top apps on the Google Play Store, the Brightest Flashlight Free app, required a number of permissions that enabled it to access private data (e.g., exact GPS location, persistent device ID). Such access does not have any relevance to the fundamental operations of the app.

Many studies in the security literature have looked at the security risks and privacy concerns due to allowing apps access to sensitive data. The privacy calculus view is commonly taken to explain user choice, wherein individuals consider both risk and reward (Smith, Dinev, & Xu, 2011). In this paper, we present a research agenda for investigating alternative theoretical lenses that can be used to more fully explain what drives users' behavior in the context of mobile app permissions requests. We derive propositions from social, economic, and cognitive perspectives.

Using multiple theoretical bases does not mean that the strategies are mutually exclusive. Instead, the selected theories provide complementary options, allowing us to determine the extent to which each theory can be used to explain the variance in user behavior. Our research question is therefore:

RQ: How strongly do social, economic, and cognitive models provide useful antecedents to mobile permissions decisions?

Each theoretical perspective is promising for examining mobile permissions decisions. Social influence research has examined how an individual's behavior can be influenced by behaviors of others. Because so many mobile tools are social in nature, personal utility (measured by comparing benefits and costs) alone might not account for enough of the variance

in the behavior of mobile users. Prospect theory was chosen because when users juggle the benefits and costs of downloading and installing an app, those gains and losses can be viewed quite differently depending on how they are presented through framing and related mechanisms Cognitive research has found several non-rational behaviors, some related to mindlessness, that have been replicated many times in the laboratory and field. Findings from these theories should complement what is already known from using a privacy calculus perspective.

In the following sections, we present an overview of the theories and constructs from social influence research, prospect theory, and several cognitive perspectives including mindlessness. We also present multiple sets of propositions which formulate our research agenda.

SOCIAL INFLUENCE

Theories of social influence are conspicuously well-suited for examining privacy behavior with socially-focused apps. The impact of social influence on privacy in general has been considered (Acquisti et al. 2012), and social influence has been shown to be an important antecedent to behavioral intentions in IS research (e.g., Venkatesh et al. 2003; Vannoy and Palvia, 2010). The theoretical underpinnings of social pressure were provided by Kelman (1958) and examined empirically in the context of TAM by Malhotra and Galletta (1999). Kelman provided three different forms of social influence, where an individual adopts a behavior through reasons of compliance, identification, or internalization. A *compliance* motive is to obtain a favorable reaction or reward, not necessarily motivated by one's beliefs. An *identification* motive is to establish or maintain the favor of a particular person or group. An *internalization* motive is to obtain intrinsic reward because the ideas and principles encompassed by the behavior align with an individual's own value system.

We next provide propositions based on compliance and identification forms of social influence. Although we do not provide propositions directly related to internalization, we do later provide propositions that consider joint impacts from social influence and framing theories, including internalization mechanisms.

Compliance

Individuals may seek to comply with a social consensus. Van Slyke et al. (2007) found that a critical mass is an essential element of social influence, which implies that an authority of some kind is formed by large numbers. Vannoy and Palvia (2010) proposed that social influence occurs when consensus is reached on performing the action, when there is cooperation with the group on performing the action, and when the authority imposed by the group dictates the legitimacy of the action. The group consensus construct is built on consensus theory, which states that if all people who are involved in a particular situation agree that an action is right, it is right. In the context of mobile apps, giving permissions upon installation can be considered a means to establish social activities and connections. Based on the compliance dimension of social influence, there are three powerful forces a group can use to impact the potential adopter of a social computing app: consensus, cooperation, and authority.

The group here refers to those with social connections with the user, not a government or legal entity. Because we are assuming that the app is available through legitimate means, and the group is assumed to not be organized with a defined hierarchy, we leave the study of authority to a future study that relaxes those assumptions. While all of these three compliance-based factors can make it more likely that a user will comply with permission requests, we will only consider consensus and cooperation. From the studies above, we propose that:

P1: Compliance with social consensus positively predicts users' acceptance of mobile app permission requests

P2: Compliance with social cooperation positively predicts users' acceptance of mobile app permission requests

Identification

Kelman (1958) explained the power of identification which involves a decision-maker who attempts to please or emulate an admired figure by adopting his or her values. There is not necessarily pressure to act, but there are visible actions that the admired person takes, which are known by the focal person. An example is provided by Dalton et al. (2003), who showed dramatic impacts on adolescents when viewing movies depicting actors smoking. An interesting four-part explanation of why celebrities have impact is provided in a meta-analysis by Hoffman and Tan (2013): People are conditioned to react positively to the advice of role models, experience cognitive dissonance if they do not, work to develop congruence with their own self-conceptions, and desire to acquire the social capital of the role models. We propose that these impacts will extend to a mobile app permissions context, where the recommendation of a role model may influence how a user reactions to mobile app permission requests. While some of this research has targeted celebrities, we assert that many individuals follow recommendations of others for loading apps, and thus accepting necessary permissions. Recommendations, opinions, and reviews of others are influential in IS acceptance contexts (e.g., Galletta et al. 1995) and in IS marketplace contexts (e.g., Pavlou and Dimoka 2006): we expect the same to hold for privacy contexts. The extent to which the recommenders are strong role models might be important, as the recommenders have demonstrated that they continue to thrive and use their devices successfully, thus creating some credibility in the subject matter.

P3: Identification with a role model who recommends usage of an app will positively influence users' acceptance of mobile app permission requests

FRAMING

Kahneman and Tversky (1979) introduced prospect theory to model decision making under risk. The basic premise is that the value of a decision follows an S-curve from losses to gains with a much steeper slope for losses than for gains. The theory has received much attention in multiple fields including finance, economics and information systems (IS). Prospect theory suggests that variations in framing an option can systematically affect the decision making of individuals. Prospect theory originally accounted for decision making under risk with positive or negative gains. Framing under risk conditions was known as risk choice framing. Later, attribute framing and goal framing were introduced to broaden understanding of framing effects under different conditions. All three types of framing are valence framing, and they result in different cognitive processing in individuals.

Goal Framing

According to goal framing, people tend to choose the option framed negatively more often than the one framed positively even if the outcome is the same. For example, women are more likely to have a mammogram when presented with negative consequences of not doing so in comparison to when presented with benefits of taking the test (Banks et al. 1995). Similarly, people tend to be more tax compliant when presented with negative consequences of non-compliance than when presented with positive benefits of tax compliance (Holler et al. 2008).

Goal framing has been examined in the IS literature as well. It has been suggested that framing security-related messages appropriately can influence behavior in individuals (Anderson and Agarwal, 2010). Authors in that study presented some individuals with a prevention-focused goal (negative frame) and others with a promotion-focused goal (positive frame). As expected, people tend to act more to enhance their security when presented with a prevention-focused goal than with a promotion-focused goal.

In the context of the present study, application owners can choose to convey benefits of features a user will receive in exchange of information access in a positive or negative frame. In line with the theory, we expect that people will provide access to their information when the resulting loss of benefits is framed negatively, compared to when it is framed positively.

P4: There will be significantly higher acceptance of a privacy-sensitive information access request when benefit information is presented with a negative frame than when presented with a positive frame.

Risk Choice Framing

Risk choice-framing effects occur when the willingness to take a risky proposition depends on whether the potential outcomes are positively or negatively framed. People tend to choose a risky option when presented with a negative frame of outcome whereas they tend to choose a less risky option with certainty when presented with a positive frame of outcome. In their famous study "Asian disease problem," Tversky and Kahnemann (1981) showed that in positive framing, people choose the treatment which will certainly save some people, whereas in negative framing, they choose an option that has uncertain outcomes.

The use of risk choice framing in privacy research is well established. It is suggested that people are less willing to share their privacy information to marketers when the rewards are uncertain and ambiguous (McCaughey and Ayers 2013). Similarly, it is observed that more individuals are willing to reject an offer of payment in exchange for reduced privacy than the number of people who will accept an economically equivalent offer to pay money in exchange for increased privacy (Acquisti et al. 2013).

In the context of our study, while asking for information access, features (in exchange for information) can be described based on their usefulness either in certain terms or with uncertainty:

P5: When asked for privacy-sensitive information access, individuals will be more likely to accept the request in exchange for features with certain usefulness if positive framing is used. Conversely, they will be more likely to accept such a request in exchange for features with uncertain usefulness if negative framing is used.

Attribute Framing

The third and final aspect of prospect theory is attribute framing. Attribute framing is a result of information coding due to framing based on a description of an event or an object. A framing which results in presenting positive aspects of an object or event, will result in positive association. Attribute framing has been used in IS research. For example, in a website quality study, it was found that the rating of perceived website quality is significantly higher in a positive frame than in a negative frame (Hartmann et al. 2008). In the negative frame it was suggested that 10% of previous users found the website difficult to use and in the positive frame subjects were told that 90% of those users found the website easy to use. Subjects perceived higher website quality when presented with positively framed information. In summary, when evaluating, a glass half full is not the same as a glass half empty.

In our study, we also expect the similar perceptions from users regarding privacy of information allowed to be utilized by mobile app owners. If presented with a positive message, people will trust the application with their data more than when information is presented in a negative frame.

P6: Users will be more likely to consent to sharing of their personal information when presented with positively framed information request than when presented with negatively framed information.

COGNITIVE MODELS

We now briefly consider two additional potent explanations for how an individual's compliance with a request may be obtained via a cognitive route. The first that we consider is

mindlessness and reactions to requests, and the second is processing of sequential-request persuasion strategies. These two explanations overlap with both social influence and framing theories.

Mindless reactions

Some forms of influence are thought to run deep within the psyche. They can be enacted "mindlessly," with individuals following a script without elaborating much on their behavior or on the choices involved for a given request. One such script is the idea of complying with polite requests. The script follows this flow: if (1) a request is polite, and if (2) a reason is given for the request, and if (3) it is not perceived to be a large request, then it may be complied with mindlessly without elaboration over the reasonableness of the requests. However, if a request is perceived to be large, then the reasonableness of the reason may be elaborated over (Abelson, 1976). A famous study testing the politeness-reasonableness script is reported in Langer et al. (1978), dubbed the "Xerox" study. In it, researchers tested compliance by asking to "cut" in front of other customers in line to use a copy machine. When a reason was given and the request was small, compliance rates were higher regardless of the reasonableness of the stated reason (e.g., an obvious reason "Can I cut in line to make a copy *because I need to make copies?*"), but when the request was large, the reasonableness of the explanation became more important for predicting compliance (e.g, "Can I cut in line *to make 500 copies…*"). The script concept is later built upon by Petty and Cacioppo's well-established elaboration likelihood model of persuasion (1986).[1]

Following these findings, in the context of mobile app permission requests, we propose that permission requests that are perceived as being small and that give a reason will be more

[1] While ELM is a powerful theoretical model, we use the theory of mindless reactions instead of ELM in our agenda because we deem that the theory of mindless reactions more directly informs the design of privacy dialogues than does ELM, which is more abstract. However, it would be useful to test the predictive power of both theories in privacy dialogue contexts in future research.

likely to be accepted than will those that are large requests or than those that do not give a reason. The difference can be explained by mindless versus mindful processing of the request.

P7: Small mobile app permissions that give a reason will be more likely to be accepted than will small mobile app permissions that do not give a reason, regardless of the reasonableness of the stated reason.

Sequential requests strategies

Compliance-gaining literature has investigated the use of sequential requesting strategies. These strategies have the requestor make a preliminary request before making a request closer to the desired outcome behavior. Two sequential requesting strategies exist: the foot-in-the-door strategy and the door-in-the-face strategy.

Foot-in-the-door strategy: The foot-in-the-door strategy (FITD) involves first making a small request. After compliance with the small request is obtained, a larger request is later made. An example is first asking someone to put a small bumper sticker on their car in support of a community cause, then later asking to put a large hideous sign supporting the same cause on the lawn (Freedman and Fraser, 1966). In studies testing this strategy, individuals who first comply with the smaller request were often more likely to comply with the second larger request than were those who were only asked the larger request (see Burger 1999 for a review).

It is thought that the theoretical explanation for the success of this strategy lies in an individual's desire to maintain a self-image of consistency. A social bond is formed through complying with the first, smaller request. To not comply with the second larger request would violate that bond, and would appear inconsistent.

Door-in-the-face strategy: The door-in-the-face strategy (DITF) is another sequential strategy that first makes an overly large request, followed up with a smaller request (Cialdini et al. 1975). As in the FITD strategy, the second request is the primary goal. The requestor expects that after

the first large request is turned down (the proverbial "door in the face"), but that this will be associated with an increased likelihood of compliance with the second request. An example is from a study asking for volunteer for a program for troubled youth. After individuals were first asked to commit to help the youth every weekend for a year, they were more likely to accept a smaller request of a one-time helping event than were individuals who were only asked the smaller request (Cialdini et al. 1975).

Relating this strategy to the theories of social influence, the initial non-compliance with the large request may raise perceptions in an individual that they have violated a social norm. This could lead to guilt. Higher compliance rates to the lesser follow-up requests may therefore be explained by guilt reduction (Millar 2002) (which also overlaps with the internalization dimension of social influence). Attribute framing may also have an effect here – the second request may seem much smaller in comparison because of the relatively larger size of the first request. The smaller perceived size of the second request may increase rates of compliance.

One way that apps request permissions is while the app is being used. For instance, an app may request location information in order to unlock some peripheral functionality. The foot-in-the-door strategy can be tested by first obtaining a smaller permission, and then afterwards requesting a larger permission. In this case, the larger permission would be the true target permission – the opening permission would be a set up. The door-in-the-face strategy would test the opposite sequence – first a permission larger than the truly targeted permission could be requested. If denied, a scaled-down permission could be requested. We summarize these approaches as follows:

P8: Permission requests that follow smaller ones will be more likely to be complied with than will stand-alone permission requests of magnitudes comparable to the second request.

P9: Permission requests that follow larger ones that have been denied will be more likely to be complied with than will stand-alone permission requests of magnitude comparable to the second request.

CONCLUSION

We have presented a mobile app permissions research agenda with propositions based on social, economic, and cognitive perspectives. This particular combination of theories and frameworks can lead to a more complex and realistic understanding of user behavior in an IS privacy context than that which is afforded by privacy calculus alone. While privacy calculus is a useful theory, we argue for the usefulness of multiple theories in explaining further variance, given that any one theory will only account partially for behavior or behaviorally-oriented responses. We believe that the promising theories listed in our agenda should be studied both separately and in conjunction with privacy calculus in future studies. We begin by studying some promising approaches in this paper, but do not intend to suggest that this would be the final study integrating multiple approaches. Furthermore, the different theories in our agenda can each uniquely inform the development of privacy dialogues. We call on future research to apply these theories using design science methodologies. Pursuit of this research agenda should lead to enrichment of the information systems privacy literature, complementing the existing literature based on privacy calculus theory, and opening new avenues for contributions to research and practice.

REFERENCES

Abelson, Robert P. *Script Processing in Attitude Formation and Decision Making*. Lawrence Erlbaum, 1976. http://psycnet.apa.org/psycinfo/1977-31627-004.

Acquisti, A., John, L. K., and Loewenstein, G. 2012. "The Impact of Relative Standards on the Propensity to Disclose," *Journal of Marketing Research* (49:2), pp. 160-174.

Acquisti, A., John, L.K., and Loewenstein, G. 2013. "What Is Privacy Worth?" *The Journal of Legal Studies* (42:2), pp. 249–274. http://doi.org/10.1086/671754

Anderson, C.L., and Agarwal, R. 2010. "Practicing Safe Computing: a Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions" *MIS Quarterly* (34:3), pp. 613–A15. http://doi.org/10.1016/j.arth.2009.05.009

Banks, Sara M., Peter Salovey, Susan Greener, Alexander J. Rothman, Anne Moyer, John Beauvais, and Elissa Epel. "The Effects of Message Framing on Mammography Utilization." *Health Psychology* 14, no. 2 (1995): 178.

Bell, K. 2015. "Google Play now has more apps than Apple's App Store, report says." *http://mashable.com/2015/01/15/google-play-more-apps-than-ios/*, accessed 4/26/2015

Burger, Jerry M. "The Foot-in-the-Door Compliance Procedure: A Multiple-Process Analysis and Review." *Personality and Social Psychology Review* 3, no. 4 (November 1, 1999): 303–25. doi:10.1207/s15327957pspr0304_2.

Cialdini, Robert B., Joyce E. Vincent, Stephen K. Lewis, Jose Catalan, Diane Wheeler, and Betty Lee Darby. "Reciprocal Concessions Procedure for Inducing Compliance: The Door-in-the-Face Technique." *Journal of Personality and Social Psychology* 31, no. 2 (1975): 206.

Cohen, T. 2014. "Backgrounder: Results of the 2014 Global Privacy Enforcement Network Sweep," *https://www.priv.gc.ca/media/nr-c/2014/bg_140910_e.asp*, accessed 4/26/2015

Clifford, C. 2014. "By 2017, the App Market Will Be a $77 Billion Industry," Entrepreneur, http://www.entrepreneur.com/article/236832, accessed 5/4/2015.

Dalton, M.A., Sargent, J.D., Beach, M.L., Titus-Ernstoff, L., Gibson, J.J., Ahrens, M B., and Heatherton, T. F. 2003. "Effect of viewing smoking in movies on adolescent smoking initiation: a cohort study," *The Lancet* (362:9380), pp. 281-285.

Davis, F.D. (1989). "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly* (13:3), pp. 319–340.

Freedman, Jonathan L., and Scott C. Fraser. "Compliance without Pressure: The Foot-in-the-Door Technique." *Journal of Personality and Social Psychology* 4, no. 2 (1966): 195.

Galletta, Dennis F., Manju Ahuja, Amir Hartman, Thompson Teo, and A. Graham Peace. "Social Influence and End-User Training." *Commun. ACM* 38, no. 7 (July 1995): 70–79. doi:10.1145/213859.214800.

Gartner. (2013). "Gartner Says Mobile App Stores Will See Annual Downloads Reach 102 Billion in 2013," *http://www.gartner.com/newsroom/id/2592315*, accessed 4/26/2015

Greenberg, A. 2014. "Mobile app study reveals privacy concerns," *SC Magazine* (September 12), *http://www.scmagazine.com/mobile%ADapp%ADstudy%ADreveals%ADprivacy%ADconcerns/printarticle/371312/*, accessed 4/26/2015

Hartmann, Jan, Alistair Sutcliffe, and Antonella De Angeli. "Towards a Theory of User Judgment of Aesthetics and User Interface Quality." *ACM Transactions on Computer-Human Interaction (TOCHI)* 15, no. 4 (2008): 15.

Hoffman, S.J., and Tan, C. 2013. "Following celebrities' medical advice: meta-narrative analysis," *BMJ* (347), f7151.

Holler, Marianne, Erik Hoelzl, Erich Kirchler, Susanne Leder, and Lucia Mannetti. "Framing of Information on the Use of Public Finances, Regulatory Fit of Recipients and Tax Compliance." *Journal of Economic Psychology* 29, no. 4 (2008): 597–611.

HP News. 2013. "HP Research Reveals Nine out of 10 Mobile Applications Vulnerable to Attack," *http://www8.hp.com/us/en/hp-news/press-release.html?id=1528865#.VT1_xSFVikp*, accessed 4/26/2015

Jordan, W. 2015. "World's most admired 2015: Angelina Jolie and Bill Gates," *https://yougov.co.uk/news/2015/01/30/most-admired-2015/*, (January 30)

Kahneman, D. and Tversky, A. 1979. "Prospect Theory: An Analysis of Decision under Risk," *Econometrica*, (47:2), pp. 263-292

Kelman, H.C. 1958. "Compliance, Identification, and Internalization: Three Processes of Attitude Change?" *Journal of Conflict Resolution*, (2:1), pp. 1–8.

Langer, Ellen J., Arthur Blank, and Benzion Chanowitz. "The Mindlessness of Ostensibly Thoughtful Action: The Role of' Placebic' Information in Interpersonal Interaction." *Journal of Personality and Social Psychology* 36, no. 6 (1978): 635.

Levin, I.P., Schneider, S.L., and Gaeth, G.J. 1998. "All Frames Are Not Created Equal: A Typology and Critical Analysis of Framing Effects," *Organizational Behavior and Human Decision Processes*, (76:2), pp. 149–188.

Liccardi, I., Pato, J., and Weitzner, D.J. 2014. "Improving User Choice Through Better Mobile Apps Transparency and Permissions Analysis," *Journal of Privacy and Confidentiality* (5:2), Article 1, pp. 1–55. Available at: http://repository.cmu.edu/jpc/vol5/iss2/1

Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J. I., and Zhang, J. 2012. "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing," *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12* (501). doi:10.1145/2370216.2370290

Malhotra, Y. and Galletta, D.F. 1999. "Extending the Technology Acceptance Model to account for social influence: theoretical bases and empirical validation," *Proceedings of the 32nd Hawaii International Conference on System Science* 00(c), pp. 1–14.

McCaughey, M., and Ayers, M.D. 2013. *Cyberactivism: Online Activism in Theory and Practice: Online Activism in Theory and Practice*. Routledge.

Millar, Murray. "Effects of a Guilt Induction and Guilt Reduction on Door in the Face." *Communication Research* 29, no. 6 (2002): 666–80.

Nielsen. 2014. "Smartphoones: So many apps, so much time," http://www.nielsen.com/us/en/insights/news/2014/smartphones-so-many-apps--so-much-time.html, accessed 4/26/2015

Petty, Richard E., and John T. Cacioppo. The Elaboration Likelihood Model of Persuasion. Springer, 1986. http://link.springer.com/chapter/10.1007/978-1-4612-4964-1_1.

Paolacci, G., Chandler, J., and Ipeirotis, P. 2010. "Running experiments on amazon mechanical turk," *Judgment and Decision Making* (5:5), pp. 411–419. doi:10.2139/ssrn.1626226

Pavlou, Paul A., and Angelika Dimoka. "The Nature and Role of Feedback Text Comments in Online Marketplaces: Implications for Trust Building, Price Premiums, and Seller Differentiation." *Information Systems Research* 17, no. 4 (2006): 392–414.

Smith, H.J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015

Statista. 2015. "Number of apps available in leading app stores as of July 2014,"http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/, accessed 4/26/2015

Sutanto, J., Palme, E., Tan, Ch., and Phang, Ch.W. 2013. "Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users," *MIS Quarterly* (37:4), pp. 1141-A5.

The Federal Trade Commission. 2014. "FTC Approves Final Order Settling Charges Against Flashlight App Creator," https://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app, accessed 4/27/2015

Tversky, Amos, and Daniel Kahneman. "The Framing of Decisions and the Psychology of Choice." *Science* 211, no. 4481 (1981): 453–58.

Tversky, A. and Kahneman, D. 1992. "Advances in prospect theory: Cumulative representation of uncertainty," *Journal of Risk and uncertainty* (5:4), pp. 297-323.

Van Slyke, C., Ilie, V., Lou, H., and Stafford, T. 2007. "Perceived critical mass and the adoption of a communication technology," *European Journal of Information Systems* (16:3), pp. 270–283. doi:10.1057/palgrave.ejis.3000680

Vannoy, S.A. and Palvia, P. 2010. "The social influence model of technology adoption," *Communications of the ACM* (53:6), p. 149. doi:10.1145/1743546.1743585

Venkatesh, V. and Davis, F.D. 2000. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Management Science* (46:2), pp. 186–204. doi:10.1287/mnsc.46.2.186.11926

Venkatesh, V., Morris, M.G., Davis, F.D., and Davis, G.B. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425-478.

Venkatesh, V., and Bala, H. 2008. "Technology acceptance model 3 and a research agenda on interventions," *Decision Sciences*, (39:2), pp. 273-315.

Young, D., Beebe, N., and Chang, F. 2012. "Prospect Theory and Information Security Investment Decisions" *AMCIS 2012 Proceedings* (July 29, 2012), Paper 8. http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/8

Zhang, F. (2012). *Assessing intrusiveness of smartphone apps* (Doctoral dissertation, Massachusetts Institute of Technology).